Highfield Priory
Independent Day School
and Nursery

Data Protection Policy

Contents

This policy should be read in conjunction with:
Confidentiality Policy
Cyber Emergency Plan
Data Breach Procedure
E-Safety Policy
Privacy Notice

Data protection is an important legal compliance issue for Highfield Priory School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the School's Privacy Notice. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

The current law (the Data Protection Act 1998) is changing on 25 May 2018 with the implementation of the General Data Protection Regulation (**GDPR**). This is an EU Regulation that is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that the personal data of pupils is at all times handled responsibly and securely.

While this new law does set out useful legal grounds in this area, in most ways this new law is strengthening the rights of individuals and placing tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law and has powers to take action for breaches of the law. **Those who are involved in the processing of personal data are obliged to comply with this policy when doing so**. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action.

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (e.g. including parents, pupils, employees).

Key data protection terms used in this data protection policy are:

- Data controller – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.

- Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
- Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- Personal information (or personal data): any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

Data Protection Lead

The School has appointed a Data Protection Officer who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

It should also be noted that data protection is the responsibility of all staff members at Highfield Priory School.

The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;

2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;

3. **Relevant** and **limited** to what is necessary for the purposes it is processed;

4. **Accurate** and kept **up to date**;

5. **Kept for no longer than is necessary** for the purposes for which it is processed; and

6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;

- documenting significant decisions and assessments about how we use personal data; and

- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is generally considered preferable to rely on another lawful ground where possible.
One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the Controller. It can be challenged by data subjects and also means the Controller is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Policy, as GDPR requires.
Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

Headline responsibilities of all staff

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School if you believe that your personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.
Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures.

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify the School Business Manager and DPO. If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be serious,

or it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the staff member's contract.

Care and data security

More generally, we require all School staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.
We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the DPO and to identity the need for (and implement) regular staff training.

Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the SBM and DPO as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them; and

- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for processing their personal data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the SBM and DPO as soon as possible.

Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. See the school's Cyber Security Guidance Pack and IT Code of Conduct for further information. As such, no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of SBM or DPO. Where a worker

is permitted to take data offsite it will need to be encrypted. Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

Summary

For example: “It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?

- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?

- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School’s culture and all its staff and representatives need to be mindful of it.”

Subject Access Request Policy (SAR)

This document sets out our policy for responding to subject access requests under the General Data Protection Act (GDPR, 2018)

It is the GDPR in the UK that explains the rights and responsibilities of those dealing with personal data. All staff are contractually bound to comply with the GDPR and other relevant the authority policies.

What is the General Data Protection Act (GDPR)?

The GDPR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The GDPR works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for specific and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individuals’ rights
- Secure
- Not transferred to other countries without adequate
- protection

Secondly, it provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Further information on the GDPR can be found in the school’s Privacy Notice and on the following website for the Information Commissioner’s Office: https://ico.org.uk/

What is the Authority's general policy on providing information?

We welcome the rights of access to information that are set out in the GDPR. We are committed to operating openly and to meeting all reasonable requests for information that are not subject to specific exemption in the Act.

How do you make a subject access request?

A subject access request is a written request for personal information (known as personal data) held about you by the school. Generally, you have the right to see what personal information we hold about you, you are entitled to be given a description of the information, what we use it for, who we might pass it onto, and any information we might have about the source of the information. However, this right is subject to certain exemptions that are set out in the GDPR.

What is personal information?

Personal data is information which is biographical or which has the individual as its focus.

Personal data is information that relates to a living individual who can be identified from the information and which affects the privacy of that individual, either in a personal or professional capacity. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

Provided the information in question can be linked to an identifiable individual, the following are likely to be examples of personal data:

- an individual's salary or other financial information
- information about an individual's family life or personal circumstances, employment or personal circumstances, any opinion about an individual's state of mind
- sensitive personal information – an individual's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual orientation, criminal record and membership of a trade union.

The following are examples of information, which will not normally be personal data:

- mere reference to a person's name, where the name is not associated with any other personal information
- incidental reference in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity
- where an individual's names appears on a document or email indicating only that it has been sent or copied to that particular individual
- the content of that document or email does not amount to personal data about the individual unless there is other information about the individual in it.

If a document has been sent by a third party, that contains information about an individual, which relates to their personal or professional life, it is personal data.

For further information, please see the school's privacy notice and data retention policy.

What do we do when we receive a subject access request?

Checking of identity

We will first check that we have enough information to be sure of your identity. Often we will have no reason to doubt a person's identity, for example, if we have regularly corresponded with you. However, if we have good cause to doubt your identity we can ask you to provide any evidence we reasonably need to confirm your identity. For example, we may ask you for a piece of information held in your records that we would expect you to know: a witnessed copy of your signature or proof of your address.

If the person requesting the information is a relative/representative of the individual concerned, then the relative/representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone under the Mental Capacity Act 2005, you must confirm your capacity to act on their behalf and explain how you are entitled to access their information. If you are the parent/guardian of a child under 16, we will need to consider whether the child can provide their consent to you acting on their behalf.

Should you make a data subject access request but you are not the data subject, you must stipulate the basis under the GDPR that you consider makes you entitled to the information.

Collation of information

We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this. We will gather any manual or electronically held information (including emails) and identify any information provided by a third party or which identifies a third party.

If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information to you unless the other party has provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed we may seek legal advice on what action we should take.

Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties not already known to the individual (e.g. the Authority employees), and edit information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document. The GDPR requires us to provide information, not documents.

Issuing our response

Once any queries around the information requested have been resolved, copies of the information in a permanent form will be sent to you except where you agree, where it is impossible, or where it would involve undue effort. In these cases, an alternative would be to allow you to view the information on screen at the school.

We will explain any complex terms or abbreviations contained within the information when it is shared with you. Unless specified otherwise, we will also provide a copy of any information that you have seen before.

What is the timeframe for responding to subject access requests?

We have 1 calendar month starting from when we have received all the information necessary to identify you, to identify the information requested, and any fee required, to provide you with the information or to provide an explanation about why we are unable to provide the information. In many cases, it will be possible to respond in advance of the 1 calendar month target and we will aim to do so where possible.

Are there any grounds we can rely on for not complying with a subject access request?

Previous request

If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined upon the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

Exemptions

The GDPR contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. Possible exemptions would be: information covered by legal professional privilege, information used for research, historical and statistical purposes, and confidential references given or received by the authority.

What if you identify an error in our records?

If we agree that the information is inaccurate, we will correct it and where practicable, destroy the inaccurate information. We will consider informing any relevant third party of the correction. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

What if you want the school to stop processing your data?

Under articles 12 and 15 of the GDPR, you can object to the school processing your data altogether, in relation to a particular purpose or in a particular way through a data subject notice. However, this only applies to certain processing activities and there is a process that you must follow when making such an objection. We must then give you written notice that either we have complied with your request, intend to comply with it or state the extent to which we will comply with it and why. This information will be given to you within 21 days of the school receiving the data subject notice. Further information on this, can be found at https://ico.org.uk/

Retention & Destruction Of Records

This policy is intended to provide information about how the school will use (or "process") personal data about individuals including: its staff; its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. Staff, parents and pupils are all encouraged to read the Privacy Notice and understand the school's obligations to its entire community.

This **retention policy** applies alongside any other information the school may provide about a particular use of personal data, for example when collecting data via an online or paper form. Highfield Priory School will generally seek to balance the benefits of keeping detailed and complete records – for the purposes of good practice, archives or general reference – with practical considerations of storage, security, space and accessibility. However, whilst independent schools are not as directly regulated as state maintained schools, there are still legal considerations in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including for safeguarding;
- disclosure requirements for potential future litigation;
- contractual obligations;
- the law of confidentiality and privacy; and (last but by no means least relevant)
- the Data Protection Act ("DPA"), to be replaced on 25th May 2018 (see below).

These will inform not only minimum and maximum retention periods, but also what to keep and importantly, who should be able to access it.
On 25th May 2018, the General Data Protection Regulation (GDPR) will take effect across the UK under a domestic Data Protection Bill.

Data Retention Periods

Below is a list of retention periods for general data files that Highfield Priory has adopted.
Some of these time periods are governed by legal requirements, such as DfE and GDPR, whilst others have been set by the school to protect both its staff and itself. A fully comprehensive list of retention periods for all files at Highfield is found within the Data Classification folder in Policies (GDPR).

File Description	Extra Information	Retention Period	Disposal Action
Governors Minutes		Permanent	
Annual Governors Reports		10 years	Secure Disposal
Head Teacher's Log Books	Data Protection	10 years	Archived if of value
SMT Minutes	Data Protection	10 years	Secure Disposal
Professional Development Plans	Data Protection	10 years	Secure Disposal
School Development Plans		10 years	Secure Disposal
Staff Sign In Book	Data Protection	6 years	Secure Disposal
Appointment Of Staff Files	Data Protection	6 months	Secure Disposal
Staff Personal File	Data Protection	10 years	Secure Disposal
Child Major Accident File	Data Protection	25 years	Secure Disposal
Staff Accident File	Data Protection	10 years	Secure Disposal
Hazardous Substance Files		50 years	Secure Disposal
Primary Pupil File	Data Protection	25 years	Secure Disposal
Child Protection Information	Data Protection	100 years	Secure Disposal
SEN Files	Data Protection	100 years	Secure Disposal
Attendance Registers	Data Protection	6 years	Secure Disposal
School Trip Consent Forms	Data Protection	6 months	Secure Disposal
School Trip Consent - Accident	Data Protection	25 years	Secure Disposal
Inspection Reports		Permanent	
Policies		Permanent	
Alumni File	Data Protection	25 years	Secure Disposal
Staff Minutes	Data Protection	10 years	Secure Disposal
Head Teacher Correspondence	Data Protection	10 years	Secure Disposal
Timesheets	Data Protection	7 years	Secure Disposal
Appraisal Records	Data Protection	7 years	Secure Disposal
Allegations Against Staff	Data Protection	10 years after retirement	Secure Disposal
SEN Correspondence	Data Protection	100 years	Secure Disposal
School Visits Risk Assessment		25 years	Secure Disposal

The above table gives a brief outline of the retention periods for general data files that are used at Highfield Priory School.

At the end of a retention period, the secure disposal process takes place on site by authorised and trained staff, who have all signed confidentiality agreements prior to conducting the disposal.

Taking, Storing and Using Images Of Pupils

- This Policy is intended to provide information to staff, pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by Highfield Priory School ("the school"). It also covers the school's approach to the use of cameras and filming equipment at school events and on school premises by parents and pupils themselves, and the media.
- It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of pupil images, including signage about the use of CCTV; and more general information about use of pupils' personal data, e.g. the school's Privacy Policy.
- Parents who accept a place for their child at the school are invited to agree to the school using images of him/her as set out in this policy, by signing a copy of the policy below or via the form attached to the school's terms and conditions. We hope parents will feel able to support the

school in using pupil images to celebrate the achievements of pupils, promote the work of the school, and for important administrative purposes such as identification and security.

- Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the Headmaster in writing. The School will always respect the wishes of parents/carers (and indeed pupils themselves) where reasonably possible, and in accordance with this policy.
- From the age of 13 onwards, parents should be aware that the law recognises pupils' own rights to decide how their personal information – including images – is used.

Use of Pupil Images in School Publications

Unless the relevant pupil or his or her parent has requested otherwise, the school will use images of its pupils to keep the school community updated on the activities of the school, and for marketing and promotional purposes, including:

I. on internal displays (including clips of moving images) on digital and conventional notice boards within the school premises;
II. in communications with the school community (parents, pupils, staff, Governors and alumni) including by email, on the school intranet and by post;
III. on the school's website and, where appropriate, via the school's social media channels, e.g. Twitter and Facebook. Such images would not normally be accompanied by the pupil's full name without permission;
IV. in the school's prospectus, and in online, press and other external advertisements for the school. Such external advertising would not normally include pupil's names.
V. The source of these images is predominantly the school's professional photographer for marketing and promotional purposes, or staff/pupils in relation to school events, sports or trips. The school will only use images of pupils in suitable dress.

Use of Pupil Images for Security

CCTV is in use on school premises, and will sometimes capture images of pupils. Images captured on the School's CCTV system are used in accordance with the school's Data Privacy Policy, and any other information or policies concerning CCTV which may be published by the school from time to time. For further information on how the school uses and stores its CCTV data, please refer to the CCTV Policy.

Use of Pupil Images in the Media

Where practicably possible, the school will always notify parents in advance when the media is expected to attend an event or school activity in which school pupils are participating, and will make every effort to ensure that any pupil whose parent or carer has refused permission for images of that pupil to be made in these circumstances are not photographed or filmed by the media.

The media normally asks for the names of the relevant pupils to go alongside the images, and these will be provided where parents have been informed about the media's visit and either parent or pupil has consented as appropriate.

Security of Pupil Images

Professional photographers and the media are accompanied at all times by a member of staff when on school premises. The school uses only reputable professional photographers and makes every effort to ensure that any images of pupils are held by them securely, responsibly and in accordance with the school's instructions.

The school takes appropriate technical and organisational security measures to ensure that images of pupils held by the school are kept securely, and protected from loss or misuse, and in particular will take reasonable steps to ensure that members of staff only have access to images of pupils held by the school where it is necessary for them to do so.

All staff are given guidance on the school's Policy on Taking, Storing and Using Images of Pupils, and on the importance of ensuring that images of pupils are made and used responsibly, only for school purposes, and in accordance with the school's policies and the law. Images of pupils in a safeguarding context are dealt with under the school's relevant safeguarding policies.

Use of Cameras and Filming Equipment (including mobile phones) by Parents

Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others.
- In particular, flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the school therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
- Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts. The school will always print a reminder in the programme of events where issues of copyright apply.
- Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.
- The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The school sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case copies of the DVDs and CDs may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

Use of Cameras and Filming Equipment by Pupils

- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of the pastoral staff.
- The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.
- The misuse of cameras or filming equipment in a way that breaches this Policy, or the school's Anti-Bullying Policy, Privacy Policy, IT Acceptable Use Policy for Pupils, or the School Rules is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

Image Storing Process For Staff

- Photographs taken on the school camera will remain on the Year Group memory card throughout the year. Memory cards will be securely backed up at the end of each academic year.
- To process photos and give access to the Social Media Coordinator for Social Media use follow the below steps.
    1. Navigate to Curriculum > Image Store > Image Store 2017
    2. Create a folder for your images with a suitable title such as ‘5D Science Nov’

3. Copy your photos from the memory card into this folder. This means they will remain on the memory card as well as be securely stored on SharePoint.
4. Email the Social Media Coordinator with a write up for the social media post and folder name.

UNDER NO CIRCUMSTANCE ARE STAFF PERMITTED TO EMAIL PHOTOS OF CHILDREN. EMAILS ARE STRAIGHTFORWARDLY HACKED. ALL PHOTOGRAPHS MUST BE STORED SECURELY ON SITE IN MEMORY CARDS OR ON SHAREPOINT SECURED SERVERS. ALL MEMORY CARDS ARE LOCKED AWAY SECURELY WITH THE DPO.

CCTV

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at ***Highfield Priory School*** (the **School**). It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV system (the System).
The System is administered and managed by the School, who act as the Data Controller. This policy will be subject to review annually, and should be read with reference to the School's Data Privacy Notice and Data Retention Policy. For further guidance, please review the Information Commissioner's (ICO) CCTV Code of Practice.

All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds. The cameras and their locations are listed here:

1	Entrance from In Drive
2	Front of School Parking
3	Exit Drive Entrance
4	Electric Gate
5	Entrance Hall and Reception
6	Playground 1 and 2
7	Main Car Park
8	Infant Quad Playground
9	Side Staff Car Parking
10	Extended Side Staff Car Park
11	Rear Staff Car Parking
12	Early Years Play Area
13	Sports Pitch
14	IP Dome

The School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

Objectives of the System

- To protect pupils, staff, volunteers, visitors and members of the public with regard to their personal safety.
- To protect the School buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the School site and deliveries and arrivals.
- To monitor staff and contractors when carrying out work duties.
- To monitor and uphold discipline among pupils in line with the [School Rules], which are available to parents and pupils on request.

Positioning

Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives.
Adequate signage has been placed in prominent positions to inform staff and pupils that they are entering a monitored area, identifying the School as the Data Controller and giving contact details for further information regarding the system.
No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.
No images of public spaces will be captured except to a limited extent at site entrances.

Maintenance

The CCTV System will be operational 24 hours a day, every day of the year.
The System Manager (defined below) will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.
The System will be checked and (to the extent necessary) serviced no less than annually.

Supervision of the System

Staff authorised by the School to conduct routine supervision of the System may include SBM, Headmaster, office staff, CSIT Coordinator, DPO, caretaker and any relevant staff on duty.
Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

Storage of Data

The day-to-day management of images will be the responsibility of **School Business Manager (SBM)** who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.
Images will be stored for up to 3 months (to cover an academic term), and automatically over-written unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.
Where such data is retained, it will be retained in accordance with the Act and our Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

Access to Images

1 Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

2 Individuals also have the right to access personal data the School holds on them (please see the Privacy Notice and Retention Policy), including information held on the System, if it has been kept. The School will require specific details including at least to time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

3 The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:

Where required to do so by the Head, the Police or some relevant statutory authority;
To make a report regarding suspected criminal behaviour;

To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;

To assist the School in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;

To data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out in 2 above;

To the School's insurance company where required in order to pursue a claim for damage done to insured property; or

In any other circumstances required under law or regulation.

4 Where images are disclosed under 3 above a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

5 Where images are provided to third parties under 3 above, wherever practicable steps will be taken to obscure images of non-relevant individuals.

Other CCTV systems

The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its Data Privacy Notice.

Complaints and queries

Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the SBM (School Business Manager).

Online Cookie and Analytics Policy

By continuing to browse the site, you are agreeing to our use of cookies as described below.
A cookie is a small file of letters and numbers that we store on your browser or the hard drive of your computer. Cookies contain information that is transferred to your computer's hard drive.
You can block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies), you may not be able to access all or parts of our site.
Highfield Priory School uses business tools embedded within Facebook and Google to advertise and celebrate school successes throughout the year.
For a more detailed description of these processes, please go to
https://www.facebook.com/business and **https://ads.google.com/intl/en_uk/home/**

We use the following cookies:

Google Analytics

By using our site, you consent to the processing of data about you by us and Google in the manner and for the purposes set out below.
We use Google Analytics, a web analytics service provided by Google, Inc. Google Analytics sets a cookie in order to evaluate visitors' use of our site.
For a detailed description about how data collected through the use of Google Analytics is used, please go to **google.co.uk/intl/en_uk/analytics/privacyoverview.html**
Google Analytics gives us control over what data we allow Google to use. We have allowed Google to use data collected through our site including visits, average session time, bounce rate and goal conversion rate.
Google stores the information collected by the cookie on servers in the United States. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf.

Data Breach

Highfield Priory School holds large amounts of personal and sensitive data.

Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This policy applies to all personal and sensitive data held by Highfield Priory School. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Please refer to Data Breach Procedure in the event of a breach.

Data Breaches at a Glance

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. All companies must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, companies must also inform those individuals without undue delay.
- Companies should ensure they have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not a company will need to notify the relevant supervisory authority and the affected individuals.
- Companies must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Definition of Data Breaches

Simply put, a data breach is the download, theft or viewing of data by someone who isn't authorized to access it. The term applies to personally identifiable data and confidential data that is access controlled.

Once data is leaked, there is effectively **no way for an organization to control its spread and use.**
It is the responsibility of all staff at Highfield Priory School to maintain a high level of data security. This not only refers to electronic files, but also to paper files that have been copied or stored incorrectly.
If you are in any doubt, please speak to the Data Protection Officer (DPO) or School Business Manager (SBM) who will be able to answer any questions regarding this area.

Staff & Customer Rights

Under the GDPR, there is a legal duty for Highfield Priory School to report personal data breaches. The ICO must be notified of data breaches without undue delay or within 72 hours, unless the breach is unlikely to be a risk to individuals.
Therefore, robust procedures for detecting, reporting and investigating data breaches need to be established to meet the GDPR requirements. Highfield Priory School has taken steps to be compliant with this requirement.
All data held by Highfield Priory School has been mapped and audited. This outlines who has access to the data, for what reasons, how/why it is stored and the full flow of where it moves throughout its 'life' at Highfield. For further information on how Highfield Priory School complies with this requirement, please read the school's Privacy, Retention and PIA policies.

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking;

The Finance and General Purposes Committee is responsible for this policy

Date Last Reviewed: September 2021

Authority

The Full Board of Governors, by delegation to sub-committees, is responsible for formulating the policies and procedures that will ensure the school continue to achieve the aims of the overall school strategy. Hence, each sub-committee has Terms of Reference and assigned responsibility for policies within that scope. The Subcommittees are: Finance and General Purpose, Health and Safety, Safeguarding, Education and Marketing.